ECHELON
The NSA's Global Spying Network

Using a system of satellites and supercomputers that recognise code-words, the US National Security Agency and its UKUSA partners keep governments, corporations and citizens under constant surveillance.

Part 1 of 2

by Patrick S. Poole © 1998/99

E-mail: pspoole@hiwaay.net
Website: http://fly.hiwaay.net/~pspoole/echelon.html

In the greatest surveillance effort ever established, the US National Security Agency (NSA) has created a global spy system, code-named ECHELON, which captures and analyses virtually every phone call, fax, e-mail and telex message sent anywhere in the world. ECHELON is controlled by the NSA and is operated in conjunction with the General Communications Headquarters (GCHQ) of the UK, the Communications Security Establishment (CSE) of Canada, the Australian Defence Security Directorate (DSD), and the General Communications Security Bureau (GCSB) of New Zealand. These organisations are bound together under a secret agreement, the UKUSA Security Agreement of 1948, whose terms and text remain under wraps even today.

The ECHELON system is fairly simple in design: position intercept stations all over the world to capture all satellite, microwave, cellular and fibre-optic communications traffic, and then process this information through the NSA's massive computer capabilities—including advanced voice recognition and optical character recognition (OCR) programs—and look for code-words or code-phrases (using what's known as the ECHELON Dictionary) that will prompt the computers to flag the message for recording and transcribing for future analysis. Intelligence analysts at each of the respective "listening stations" maintain separate keyword lists for them to analyse any conversation or document flagged by the system, which is then forwarded to the respective intelligence agency headquarters that requested the intercept.

But apart from directing their ears towards terrorists and rogue states, ECHELON is also being used for purposes well outside its original mission. The regular discovery of domestic surveillance targeted at American civilians for reasons of "unpopular" political affiliation or for no probable cause at all—in violation of the First, Fourth and Fifth Amendments of the US Constitution—is consistently impeded by very elaborate and complex legal arguments and privilege claims by the intelligence agencies and the US Government. The guardians and caretakers of our liberties, our duly elected political representatives, give scarce attention to these activities, let alone to the abuses that occur under their watch.

Among the activities that the ECHELON targets are:

• **Political spying:** Since the close of World War II, the US intelligence agencies have developed a consistent record of trampling the rights and liberties of the American people. Even after the investigations into the domestic and political surveillance activities of the agencies that followed in the wake of the Watergate fiasco, the NSA continues to target the political activity of "unpopular" political groups and our duly elected representatives.

One whistleblower charged, in a 1988 Cleveland *Plain Dealer* interview, that while she was stationed at the Menwith Hill facility in the 1980s she heard real-time intercepts of South Carolina Senator Strom Thurmond. A former Maryland Congressman, Michael Barnes, claimed in a 1995 Baltimore *Sun* article that under the Reagan Administration his phone calls were regularly intercepted—something he discovered only after reporters had been passed transcripts of his conversations by the White House. One of the most shocking revelations came to light after several GCHQ officials became concerned about the targeting of peaceful political groups, and told the London *Observer* in 1992 that the ECHELON Dictionaries targeted Amnesty International, Greenpeace and even Christian ministries.

• **Commercial espionage:** Since the demise of communism in Eastern Europe, the intelligence agencies have searched for a new justification for their surveillance capability in order to protect their prominence and their bloated budgets. Their solution was to

redefine the notion of "national security" to include economic, commercial and corporate concerns. The Office of Intelligence Liaison was created within the US Department of Commerce to forward intercepted materials to major US corporations. In many cases, the beneficiaries of this commercial espionage effort are the very companies that helped the NSA develop the systems that power the ECHELON network. This incestuous relationship is so strong, that sometimes this intelligence information is used to push other American manufacturers out of deals in favour of these mammoth US defence and intelligence contractors who frequently are the source of major cash contributions to both political parties.

While signals intelligence technology was helpful in containing and eventually defeating the Soviet empire during the Cold War, what was once designed to target a select list of communist countries and terrorist states is now indiscriminately directed against virtually every citizen in the world. The European Parliament is now asking whether the ECHELON communications interceptions violate the sovereignty and privacy of citizens in other countries. In some cases, such as at the NSA's Menwith Hill station in England, surveillance is conducted against citizens on their own soil and with the full knowledge and cooperation of their government.

This report suggests that Congress pick up its long-neglected role as watchdog of the constitutional rights and liberties of the American people, instead of play its current role as lap dog to the US intelligence agencies. Congressional hearings, similar to the Church and Rockefeller Committee hearings held in the mid-1970s, ought to be held to find out to what extent ECHELON targets the personal, political, religious and commercial communications of US citizens.

The late US Senator Frank Church warned that the technology and capability embodied in the ECHELON system represent a direct threat to the liberties of the American people. Left unchecked, ECHELON could be used by either the political elite or the intelligence agencies themselves as a tool to subvert the civil protections of the Constitution and to destroy representative government in the United States.

Despite the disintegration of communism in the former Soviet Union and throughout Eastern Europe, the secretive NSA continues to grow at an exponential rate in terms of budget, manpower and spying abilities.

ECHELON AND THE UKUSA AGREEMENT

The culmination of the Cold War conflict brought home hard realities for many military and intelligence agencies who were dependent upon the confrontation for massive budgets and little civilian oversight. World War II Allied political and military alliances had quickly become intelligence alliances in the shadow of the Iron Curtain that descended upon Eastern Europe after the war.

But for some intelligence agencies, the end of the Cold War just meant a shift in mission and focus, not a loss of manpower or financial resources. One such US governmental organisation is the National Security Agency. Despite the disintegration of communism in the former Soviet Union and throughout Eastern Europe, the secretive NSA continues to grow at an exponential rate in terms of budget, manpower and spying abilities. Other countries have noticed the rapid growth of NSA resources and facilities around the world, and have decried the extensive spying upon their citizens by the United States.

A preliminary report, released by the European Parliament in January 1998, detailed research conducted by independent researchers that uncovered a massive US spy technology network that routinely monitors telephone, fax and e-mail information on citizens all over the world, but particularly in the European Union (EU) and Japan. Titled "An Appraisal of Technologies of Political Control",[1] this report, issued by the Scientific and Technological Options Assessment (STOA) Committee of the European Parliament, caused a tremendous stir in the establishment Press in Europe. At least one major US media outlet, the *New York Times*,[2] also covered the issuance of the report.

The STOA report also exposed a festering sore-spot between the US and its EU allies. The widespread surveillance of citizens in EU countries by the NSA has been known and discussed by European journalists since 1981. The name of the system in question is ECHELON, and it is one of the most secretive spy systems in existence.

ECHELON is actually a vast network of electronic spy stations located around the world and maintained by five countries: the USA, the UK, Canada, Australia and New Zealand. These countries, bound together in a still-secret agreement, UKUSA [pronounced "you-koo-za"], spy on each other's citizens by intercepting and gathering electronic signals of almost every telephone call, fax and e-mail message transmitted around the world daily. These signals are fed through the NSA's massive supercomputers that look for certain keywords called the ECHELON Dictionaries.

Most of the details of this mammoth spy system—and the UKUSA agreement that supports it—remain a mystery. What is known of ECHELON is the result of the efforts of journalists and researchers around the world, who have laboured for decades to uncover the operations of our governments' most secret systems. The 1996 publication of New Zealand journalist Nicky Hager's book, *Secret Power: New Zealand's Role in the International Spy Network*,[3] provided the most detailed look at the system and inflamed interest in ECHELON as well as the debate regarding its propriety.

This paper examines the expanse of the ECHELON system, along with the intelligence agreements and exchanges that support it. The operation of ECHELON serves the NSA's goal of spying on the citizens of other countries, while also allowing them to circumvent the prohibition on spying on US citizens. ECHELON is not only a gross violation of the US Constitution, but it violates the goodwill of the United States' allies and threatens the privacy of innocent civilians around the world. The existence and expansion of ECHELON is a foreboding omen regarding the future of constitutional liberties. If a US Government agency can willingly violate the most basic components of the Bill of Rights without so much as congressional oversight and approval, we have reverted from a republican form of government to tyranny.

THE UKUSA PARTIES

The success of the Allied military effort in World War II was due in no small part to successes in gathering enemy intelligence information and cracking those military and diplomatic messages. In addition, the Allied forces were able to create codes and encryption devices that effectively concealed sensitive information from prying Axis-power eyes. These coordinated signal

intelligence (SIGINT) programs kept Allied information secure and left the enemies vulnerable.

But at the close of the conflict, a new, threatening power—the Soviet Union—was beginning to provoke the Cold War by enslaving Eastern Europe. These signal intelligence agencies now had a new enemy towards which to turn their electronic eyes and ears to ensure that the balance of power could be maintained. The volleys of electronic hardware and espionage that would follow for 40 years would be the breeding ground of the ECHELON spy system.

The diplomatic foundation that was the genesis of ECHELON is the UKUSA agreement. The agreement has its roots in the BRUSA COMINT (communications intelligence) alliance formed in the early days of World War II and ratified on 17 May 1943 by the United Kingdom and the United States of America.[4] The Commonwealth SIGINT Organisation, formed in 1946–47, brought together the postwar intelligence agencies of the UK, Canada, Australia and New Zealand.[5] Forged in 1947 between the US and UK, the still-secret UKUSA agreement defined the relations between the SIGINT departments of those various governments. Direct agreements between the US and these agencies also define the intricate relationships of these organisations.

Forged in 1947 between the US and UK, the diplomatic foundation that was the genesis of ECHELON is the still-secret UKUSA agreement.

Foremost among those agencies is the US National Security Agency (NSA) which represents the American interest. The NSA is designated as the "First Party to the [UKUSA] Treaty". The UK Government Communications Headquarters (GCHQ) signed the UKUSA agreement on behalf of the UK and its Commonwealth SIGINT partners. This brought Australia's Defence Signals Directorate (DSD), Canada's Communications Security Establishment (CSE) and New Zealand's Government Communications Security Bureau (GCSB) into the arrangement. While these agencies are bound by additional direct agreements with the US and each other, these four countries are considered the "Second Parties to the Treaty". Third Party members include Germany, Japan, Norway, South Korea and Turkey. There are sources that indicate China may also be included in this group, on a limited basis.[6]

THE NATIONAL SECURITY AGENCY

The prime mover in the UKUSA arrangement is undeniably the US National Security Agency. The majority of funds for joint projects and facilities (discussed below) as well as the directions for intelligence-gathering operations are issued primarily through the NSA. The participating agencies frequently exchange personnel, divide up intelligence collection tasks and establish common guidelines for classifying and protecting shared information. However, the NSA utilises its role as the largest spy agency in the world to have its international intelligence partners do its bidding.

President Harry Truman established the NSA in 1952 with a presidential directive that remains classified to this day. The US Government did not acknowledge the existence of the NSA until 1957. Its original mission was to conduct the signal intelligence (SIGINT) and communications security (COMSEC) for the United States. President Ronald Reagan added the tasks of information systems security and operations security training in 1984 and 1988 respectively. A 1986 law charged the NSA with supporting combat operations for the Department of Defense.[7]

Headquartered at Fort George Meade, located between Washington, DC, and Baltimore, Maryland, the NSA boasts the most enviable array of intelligence equipment and personnel in the world. The NSA is the largest global employer of mathematicians, featuring the best teams of codemakers and codebreakers ever assembled. The codebreakers' job is to crack the encryption codes of foreign and domestic electronic communications, forwarding the revealed messages to their enormous team of skilled linguists who can review and analyse messages in over 100 languages. The NSA is also responsible for creating the encryption codes that protect the US Government's communications.

In its role as gang leader for UKUSA, the NSA is primarily involved with creating new surveillance and codebreaking technology, directing the other cooperating agencies to their targets and providing them with training and tools to intercept, process and analyse enormous amounts of signals intelligence. By possessing what is arguably the most technologically advanced communications, computer and codebreaking equipment of any government agency in the world, the NSA serves as a competent and capable taskmaster for UKUSA.

THE ECHELON NETWORK

The vast network created by the UKUSA community stretches across the globe and into the reaches of space. Land-based intercept stations, intelligence ships sailing the seven seas and top-secret satellites whirling 20,000 miles overhead all combine to empower the NSA and its UKUSA allies with access to the entire global communications network. Very few signals escape its electronic grasp.

Having divided up the world among the UKUSA parties, each agency directs its electronic "vacuum-cleaner" equipment towards the heavens and the ground to search for the most minute communications signals that traverse the system's immense path. The NSA facilities in the US cover the communications signals of both American continents; the GCHQ in Britain is responsible for Europe, Africa and Russia (west of the Ural Mountains); the DSD in Australia assists in SIGINT collection in Southeast Asia, the southwest Pacific Ocean and eastern Indian Ocean areas; the GSCB in New Zealand is responsible for southern Pacific Ocean collections, particularly the South Pacific island nations group; and the CSE in Canada handles interception of additional northern Russian, northern European and American communications.[8]

The backbone of the ECHELON network are the massive listening and reception stations directed at the Intelsat and Inmarsat satellites that are responsible for the vast majority of phone and fax communications traffic within and between countries and continents. The 20 Intelsat satellites follow a geostationary orbit locked onto a particular point on the equator.[9] These satellites carry primarily civilian traffic, but they do additionally carry diplomatic and governmental communications that are of particular interest to the UKUSA parties.

Originally, only two stations were responsible for Intelsat intercepts: Morwenstow in England, and Yakima in the US state of Washington. However, when the Intelsat 5 series was replaced with the Intelsat 701 and 703 satellites—which had much more precise transmission beams that prohibited reception of southern hemisphere signals from the Yakima base in the northern

hemisphere—additional facilities were constructed in Australia and New Zealand.[10]

Today, the Morwenstow station directs its ears towards the Intelsats traversing the atmosphere above the Atlantic and Indian oceans and transmitting to Europe, Africa and western parts of Asia. The Yakima station, located in the grounds of the Yakima Firing Station, targets the Far East and Pacific Ocean communications in the northern hemisphere. Another NSA facility at Sugar Grove, West Virginia, covers traffic for the whole of North and South America. A DSD station at Geraldton, WA, Australia, and the GCSB facility at Waihopai, New Zealand, cover Asia, the South Pacific countries and the Pacific Ocean. An additional station on Ascension Island in the Atlantic Ocean between Brazil and Angola is suspected of covering the Atlantic Intelsat's southern hemisphere communications.[11]

Non-Intelsat satellites are monitored from these same stations, as well as from bases in: Menwith Hill, England; Shoal Bay, near Darwin, Australia; Leitrim, Canada; Bad Aibling, Germany; and Misawa, Japan. These satellites typically carry Russian and regional communications.[12] It is known that the Shoal Bay facility targets a series of Indonesian satellites, and that the Leitrim station intercepts communications from Latin American satellites, including the Mexican telephone company's Morelos satellite.[13]

Another major support for the ECHELON system is the US spy satellite network and its corresponding reception bases scattered about the UKUSA empire.

Several dozen other radio listening posts operated by the UKUSA allies dot the globe as well, located at military bases on foreign soil and in remote locations. These stations played a critical role in the time prior to the development of satellite communications because much of the world's communications traffic was transmitted on radio-frequency bands.

Particularly in the high-frequency (HF) range, radio communications continue to serve an important purpose, despite the widespread use of satellite technology, because their signals can be transmitted to military ships and aircraft across the globe. Shorter range, very high frequencies (VHF) and ultra high frequencies (UHF) are also used for tactical military communications within national borders. Major radio facilities in the UKUSA network include: Tangimoana, New Zealand; Bamaga, Cape York, Australia; and the joint NSA/GCHQ facility at the Indian Ocean atoll, Diego Garcia.[14] A separate high-frequency direction-finding (HFDF) network intercepts communications signals for the unique purpose of locating the position of ships and aircraft. While these stations are not actually involved in the analysis of messages, they play a critical role in monitoring the movements of mobile military targets.

The Canadian CSE figures prominently in the UKUSA HFDF network, code-named CLASSIC BULLSEYE, hosting a major portion of the Atlantic and Pacific stations that monitored Soviet ship and submarine movements during the Cold War. Stations from Kingston and Leitrim in Ontario, to Gander, Newfoundland, on the Atlantic side, from Alert in the Northwest Territories (located at the northernmost tip of Canada on the Arctic Ocean, and able to listen to the Russian submarine bases at Petropavlovsk and Vladivostok) and finally to Masset, British Columbia, in the Pacific, monitor shipping and flight lanes under the direction of the NSA.[15] The CSE also maintains a small contingent at Lackland Air Force Base in San Antonio, Texas, which probably monitors Latin American communications targets.

Another major support for the ECHELON system is the US spy satellite network and its corresponding reception bases scattered about the UKUSA empire. These space-based electronic communications "vacuum cleaners" pick up radio, microwave and cellphone traffic on the ground. They were launched by the NSA in cooperation with its sister spy agencies, the National Reconnaissance Office (NRO) and the Central Intelligence Agency (CIA). The Ferret series of satellites in the 1960s, the Canyon, Rhyolite and Aquacade satellites in the 1970s, and the Chalet, Vortex, Magnum, Orion and Jumpseat series of satellites in the 1980s have given way to the new and improved Mercury, Mentor and Trumpet satellites during the 1990s (see table 1).

These surveillance satellites act as giant scoops, picking up electronic communications, cellphone conversations and various

Table I. US Spy Satellites in Current Use

Satellite	No.	Orbit	Manufacturer	Purpose
Advanced KH-11	3	200 miles	Lockheed Martin	5-inch-resolution spy photographs
LaCrosse Radar Imaging	2	200–400 miles	Lockheed Martin	3-10-foot-resolution spy photographs
Orion/Vortex	3	22,300 miles	TRW	Telecom surveillance
Trumpet	2	200–22,300 miles	Boeing	Surveillance of cellular phones
Parsae	3	600 miles	TRW	Ocean surveillance
Satellite Data Systems	2	200–22,300 miles	Hughes	Data relay
Defence Support Program	4+	22,300 miles	TRW/Aerojet	Missile early warning
Defence Meteorological Support Program	2	500 miles	Lockheed Martin	Meteorology, nuclear blast detection

(Source: MSNBC[16])

radio transmissions. The downlink stations that control the operations and targeting of these satellites are under the exclusive control of the United States, despite their location on foreign military bases. The two primary downlink facilities are at Menwith Hill, England, and Pine Gap, central Australia.

THE MENWITH HILL FACILITY

The Menwith Hill facility is located in North Yorkshire, England, near Harrogate. The important role that Menwith Hill plays in the ECHELON system was recognised by the recent European Parliament STOA report:

> *Within Europe, all e-mail, telephone and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland via the strategic hub of London, then by satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North Yorks Moors of the UK.*[17]

The existence and importance of the facility was first brought to light by British journalist/researcher Duncan Campbell in 1980.[18] Today, it is the largest spy station in the world, with over 25 satellite receiving stations and 1,400 American NSA personnel working with 350 UK Ministry of Defence staff on site.

After revelations that the facility coordinates surveillance for the vast majority of the European continent, the base has become a target for regular protests organised by local peace activists. It has also become the target of intense criticism by European government officials who are concerned about the vast network of civilian surveillance and economic espionage conducted from the station by the United States.[19]

... at least three major DOMESTIC fibre-optic telephone trunk lines—each capable of carrying 100,000 calls simultaneously—were wired through Menwith Hill, allowing the NSA to tap into the very heart of the British Telecom network.

The beginnings of Menwith Hill go back to December 1951, when the US Air Force and British War Office signed a lease for land that had been purchased by the British Government. The NSA took over the lease of the base in 1966 and has continued to build up the facility ever since.

Up until the mid-1970s, Menwith Hill was used for intercepting international leased carrier (ILC) communications and non-diplomatic communications (NDC). Having received one of the first sophisticated IBM computers in the early 1960s, Menwith Hill was also used to sort through the voluminous unenciphered telex communications, which consisted of international messages, telegrams and telephone calls from the government, business and civilian sectors, in the search for anything of political, military or economic value.[20]

The addition of the first satellite intercept station at Menwith Hill in 1974 raised the base's prominence in intelligence-gathering. Eight large satellite communications dishes were installed during that phase of construction. Several satellite gathering systems now dot the facility:[21]

STEEPLEBUSH – Completed in 1984, this $160 million system expanded the satellite surveillance capability and mission of the spy station beyond the bounds of the installation that began in 1974.

RUNWAY – Running east and west across the facility, this system receives signals from the second-generation geosynchronous Vortex satellites and gathers miscellaneous communications traffic from Europe, Asia and the former Soviet Union. The information is then forwarded to the Menwith Hill computer systems for processing. RUNWAY may have recently been replaced or complemented by another system, RUTLEY.

PUSHER – This is an HFDF system that covers the HF frequency range between 3 MHz and 30 MHz—radio transmissions from CB radios, walkie-talkies and other radio devices. Military, embassy, maritime and air flight communications are the main targets of PUSHER.

MOONPENNY – Uncovered by British journalist Duncan Campbell in the 1980s, this system is targeted at the communication relay satellites belonging to other countries, as well as the satellites over the Atlantic and Indian oceans.

KNOBSTICKS I and II – The purpose of these antennae arrays is unknown, but they probably target military and diplomatic traffic throughout Europe.

GT-6 – A new system installed at the end of 1996, GT-6 is believed to be the receiver for the third generation of geosynchronous satellites termed Advanced Orion or Advanced Vortex. A new polar orbit satellite called Advanced Jumpseat may be monitored from here as well.

STEEPLEBUSH II – An expansion of the 1984 STEEPLEBUSH system, this computer system processes information collected from the RUNWAY receivers that gather traffic from the Vortex satellites.

SILKWORTH – Constructed by Lockheed Corporation, the main computer system for Menwith Hill processes most of the information received by the various reception systems.

One shocking revelation about Menwith Hill came to light in 1997 during the trial of two women peace campaigners appealing their convictions for trespassing at the facility. In documents and testimony submitted by British Telecom in the case, Mr R.G. Morris, BT's head of Emergency Planning, revealed that at least three major domestic fibre-optic telephone trunk lines—each capable of carrying 100,000 calls simultaneously—were wired through Menwith Hill,[22] allowing the NSA to tap into the very heart of the British Telecom network. Judge Jonathan Crabtree rebuked British Telecom over his revelations and prohibited Mr Morris from giving any further testimony in the case for "national security" reasons.

According to Duncan Campbell, the secret spying alliance between Menwith Hill and British Telecom began in 1975 with a coaxial connection to the British Telecom microwave facility at Hunter's Stone, four miles away from Menwith Hill—a connection maintained even today.[23]

Additional systems—TROUTMAN, ULTRAPURE, TOTALISER, SILVERWEED, RUCKUS et al.—complete the monumental SIGINT collection efforts at Menwith Hill.

Directing its electronic vacuum-cleaners towards unsuspecting communications satellites in the skies, receiving signals gathered by satellites that scoop up the most minute signals on the ground, listening in on the radio communications throughout the air or plugging into the ground-based telecommunications network, Menwith Hill—alongside its sister stations at Pine Gap, Australia, and Bad Aibling, Germany—represents the comprehensive effort of the NSA, with its UKUSA allies, to make sure that no communications signal escapes its electronic net.

THE ECHELON DICTIONARIES

The extraordinary ability of ECHELON to intercept most of the communications traffic in the world is breathtaking in its scope. And yet the power of ECHELON resides in its ability to decrypt, filter, examine and codify these messages into selective categories for further analysis by intelligence agents from the various UKUSA agencies.

As the electronic signals are brought into the station, they are fed through the massive computer systems, such as Menwith Hill's SILKWORTH, where voice recognition, optical character recognition (OCR) and data information engines get to work on the messages. These programs and computers transcend state-of-the-art; in many cases, they are well into the future.

MAGISTRAND is part of the Menwith Hill SILKWORTH supercomputer system that drives the powerful keyword search programs.[24] One tool used to sort through the text of messages, PATHFINDER (manufactured by the UK company, Memex),[25] sifts through large databases of text-based documents and messages looking for keywords and key phrases based on complex algorithmic criteria. Voice recognition programs convert conversations into text messages for further analysis. One highly advanced system, VOICECAST, can target an individual's voice pattern so that every call that person makes is transcribed for future analysis.

Processing millions of messages every hour, the ECHELON systems churn away 24 hours a day, seven days a week, looking for targeted keyword series, phone and fax numbers, and specified voiceprints. It is important to note that very few messages and phone calls are actually transcribed and recorded by the system. The vast majority are filtered out after they are read or listened to by the system. Only those messages that produce keyword "hits" are tagged for future analysis. Again, it is not just the ability to collect the electronic signals that gives ECHELON its power; it is the tools and technology that are able to whittle down the messages to only those that are important to the intelligence agencies.

Each station maintains a list of keywords (the Dictionary) designated by each of the participating intelligence agencies. A Dictionary Manager from each of the respective agencies is responsible for adding, deleting or changing the keyword search criteria for their Dictionaries at each of the stations.[26] Each station Dictionary is given a code-word, such as COWBOY for the Yakima facility and FLINTLOCK for the Waihopai facility.[27] These code-words play a crucial identification role for the analysts who eventually look at the intercepted messages.

Each message flagged by the ECHELON Dictionaries as meeting the specified criteria is sorted by a four-digit code representing the source or subject of the message (such as 5535 for Japanese diplomatic traffic, or 8182 for communications about distribution of encryption technology)[28] as well as the date, time and station code-word. Also included in the message headers are the code-names for the intended agency: ALPHA-ALPHA (GCHQ), ECHO-ECHO (DSD), INDIA-INDIA (GCSB), UNIFORM-UNIFORM (CSE), and OSCAR-OSCAR (NSA). These messages are then transmitted to each agency's headquarters via a global computer system, PLATFORM,[29] that acts as the information nervous system for the UKUSA stations and agencies.

Every day, analysts located at the various intelligence agencies review the previous day's product. As it is analysed, decrypted and translated, it can be compiled into the different types of analysis: reports, which are direct and complete translations of intercepted messages; "gists", which give basic information on a series of messages within a given category; and summaries, which are compilations from both reports and gists.[30] These are then given classifications: MORAY (secret), SPOKE (more secret than MORAY), UMBRA (top secret), GAMMA (Russian intercepts), and DRUID (intelligence forwarded to non-UKUSA parties). This analysis product is the *raison d'être* of the entire ECHELON system. It is also the lifeblood of the UKUSA alliance.

NATIONAL SECURITY & SURVEILLANCE OF CITIZENS

The ECHELON system is the product of the Cold War conflict—an extended battle replete with heightened tensions that teetered on the brink of annihilation, and the diminished hostilities of *détente* and *glasnost*. Vicious cycles of mistrust and paranoia between the United States and the Soviet empire fed the intelligence agencies to the point that, with the fall of communism throughout Eastern Europe, the intelligence establishment began to grasp for a mission that justified its bloated existence.

But the rise of post-modern warfare—terrorism—gave the establishment all the justification it needed to develop an even greater ability to spy on its enemies, its allies and its own citizens. ECHELON is the result of those efforts. The satellites that fly thousands of miles overhead and yet can spy out the most minute details on the ground; the secret submarines that troll the ocean floors and tap into undersea communications cables[31]—all power the efficient UKUSA signals intelligence machine.

In the US there is a concerted effort by intelligence agency heads, federal law enforcement officials and congressional representatives to defend the capabilities of ECHELON.

In the United States there is a concerted effort by intelligence agency heads, federal law enforcement officials and congressional representatives to defend the capabilities of ECHELON. Their persuasive arguments point to the tragedies seen in the bombings in Oklahoma City and the World Trade Center in New York City. The vulnerability of Americans abroad, as recently seen in the bombing of the American Embassy in Dar es Salaam, Tanzania, and in Nairobi, Kenya, emphasises the necessity of monitoring those forces around the world that would use senseless violence and terror as political weapons against the US and its allies.

Intelligence victories add credibility to the arguments that defend such a pervasive surveillance system. The discovery of missile sites in Cuba in 1962, the capture of the *Achille Lauro* terrorists in 1995, the discovery of alleged Libyan involvement in the bombing of a Berlin discotheque that killed one American (resulting in the 1996 bombing of Tripoli), and countless other incidents that have been averted (which are now covered by the silence of indoctrination vows and top-secret classifications), all point to the need for comprehensive signals intelligence gathering for the national security of the United States.

But despite the real threats and dangers to the peace and protection of American citizens at home and abroad, the US Constitution is quite explicit in limiting the scope and powers of government.

Editor's Note:
In our next issue, part 2 of this article exposes how the ECHELON network is being used for political and commercial spying.

Continued on page 85

ECHELON: The NSA's Global Spying Network

Continued from page 24

Endnotes

1. Wright, Steve, "An Appraisal of Technologies of Political Control", Scientific and Technological Options Assessment Committee, European Parliament, Luxembourg, January 6, 1998.
2. Giussani, Bruno, "European Study Paints a Chilling Portrait of Technology's Uses", *New York Times*, February 24, 1998.
3. Hager, Nicky, *Secret Power: New Zealand's Role in the International Spy Network*, Craig Potton Publishing, Nelson, New Zealand, 1996.
4. Ball, Desmond and Richelson, Jeffrey, *The Ties That Bind: Intelligence Cooperation between the UKUSA Countries*, Allen & Unwin, Boston, 1985, pp. 137-8.
5. Ibid., pp. 142-143.
6. Hager, ibid., p. 40; see note 3.
7. National Security Agency, *About the NSA*, FAQ.
8. Ball and Richelson, ibid., p. 143.
9. The coverage areas of the various Intelsat satellites can be found at website <www.intelsat.com/cmc/connect/globlmap.htm>.
10. Hager, ibid., p. 28.
11. Ibid., p. 35.
12. Ibid.
13. Campagna, Marco, "Un Système de Surveillance Mondiale", *Cahiers de Television*, CTV-France, June 1998; Hum, Peter, "I Spy", Ottawa *Citizen*, May 10, 1997.
14. Hager, ibid., pp. 35-36, p. 150; Ball and Richelson, ibid., pp. 204-207.
15. Frost, Mike and Graton, Michel, *Spyworld: How CSE Spies on Canadians and the World*, Seal/McClelland-Bantam, Toronto, 1995, p. 35.
16. Windrem, Robert, "Spy Satellites Enter New Dimension", MSNBC and NBC News, August 8, 1998.
17. Wright, ibid., p. 19.
18. Campbell, Duncan and Melvern, Linda, "America's Big Ear on Europe", *New Statesman*, July 18, 1980, pp. 10-14.
19. Davies, Simon, "EU Simmers over Menwith Listening Post", *Telegraph*, London, July 16, 1998.
20. Rufford, Nicholas, "Spy Station F83", *Sunday Times*, London, May 31, 1998.
21. Campbell, Duncan, "Somebody's Listening", *The New Statesman*, August 12, 1988, pp. 10-12; "The Hill", *Dispatches*, BBC Channel 4, October 6, 1993 (transcript provided by Duncan Campbell); Wirbel, Loring, "Space: Intelligence Technology's Embattled Frontier", *Electronic Engineering Times*, April 22, 1997; Rufford, Nicholas, "Cracking the Menwith Codes", *Sunday Times*, London, May 31, 1998.
22. Campbell, Duncan, "BT Condemned for Listing Cables to US SIGINT Station", September 4, 1997.
23. Ibid.; Rufford, ibid.
24. Mentioned in "The Hill", *Dispatches*.
25. Wright, ibid. Memex maintains a website describing their defence and intelligence products and contracts: <www.memex.co.uk/prod/intelligence/comm.html>.
26. Hager, ibid., p. 49.
27. Ibid., pp. 165-166.
28. Ibid., p. 44.
29. Bamford, James, *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*, Penguin Books, New York, 1983, pp. 138-139.
30. Hager, ibid., p. 45.
31. Ball and Richelson, ibid., pp. 223-224.

Additional References

- Poole, Patrick, "Inside America's Secret Court: The Foreign Intelligence Surveillance Court" (Privacy Paper).
- "Lawmakers Raise Questions about International Spy Network", *New York Times*, May 27, 1999.
- "How the United States Spies on Us All", *Le Monde Diplomatique*, January 1999.
- "EU may Investigate US Global Spy Network", *Federal Computer Week*, November 17, 1998.
- "ECHELON: Surveilling Surveillance", *Inter@ctive Week*, November 16, 1998.
- "Push for Hearings on ECHELON", WorldNetDaily, November 12, 1998.
- "Spying on the Spies", *Wired*, October 27, 1998.
- "Putting NSA Under Scrutiny", Baltimore *Sun*, October 18, 1998.
- Bryce, Susan, "Silent Partners: The UKUSA Agreement", *NEXUS* 2/27, Aug-Sept 1995.

About the Author:

Patrick S. Poole is a lecturer in government and economics at Bannockburn College in Franklin, Tennessee, USA, having previously served as Deputy Director of the Center for Technology Policy in Washington, DC. He contributes frequently to several publications on the topics of privacy and civil liberties.